Guidelines for Managing E-Mail in Kentucky Government[1]

I. Introduction

Electronic Mail (e-mail) is an important communication tool for conducting government business in the Commonwealth of Kentucky. Increasingly, government agencies use e-mail systems to distribute memos, circulate drafts, disseminate directives, transfer official documents, send external correspondence, and support various aspects of government operations. Well-designed and properly managed e-mail systems expedite business communications, eliminate paperwork, and automate routine office tasks.[2] More advanced office systems being contemplated by state and local government agencies will employ mail frameworks in more complex work flow and document management processes, and move more government record keeping to online computerized systems.

Because of the dynamic and often informal nature of e-mail, many questions have arisen over the official and legal status of e-mail messages. For state agencies, two existing Enterprise policies, (1) “Status of E-mail as a Public Record” and (2) “Internet and Electronic Mail Acceptable Use Policy (CIO-060),” clarify the public record status of e-mail messages and set broad parameters for the management and acceptable use of e-mail in the executive branch of state government. These guidelines were developed to complement Enterprise Architecture Standard 4060, “Recordkeeping – Electronic Mail,” clarify agency responsibilities in meeting the requirements of the policies and standard mentioned above. For local governments, and state agencies that do not follow the Enterprise IT Architecture, these guidelines represent best practices that are designed to assist agencies in effectively and efficiently managing their e-mail records. While local governments are not bound by the Enterprise Policies and Standards, the Internet and Electronic Mail Acceptable Use Policy (CIO-060) can be a model for local agencies to base their own policies and standards on.

Since e-mail meets the statutory definition of a public record in Kentucky, it is subject to management requirements which may not be obvious. For example, electronic mail may be subject to open records requests, yet its users may have inappropriate expectations of privacy and informality; mail may be destroyed inappropriately; or it may be accumulating in systems when it should more properly be destroyed after it no longer has value to the agency. Case law shows that electronic mail certainly is discoverable under actions brought against the government, and its inappropriate retention therefore brings risk. This document will provide agencies with current guidelines and best practices to assist in the management of their e-mail records.

---

[1] This document is issued by the Kentucky Department for Libraries and Archives to assist public employees with the management of their e-mail and was developed by department staff, with the advice and assistance of members of an informal, joint interagency body, the Electronic Records Working Group.

[2] “Managing Records in E-Mail Systems,” New York State Archives and Records Administration (NYSARA) 1995.

II. Definitions

The very term “e-mail” is confusing because it is used synonymously to mean both the e-mail system and the messages distributed by the system. It can also be used to describe the action of sending or receiving an e-mail message. For the purposes of this document, the word “e-mail” is distinguished by the following terms:

E-mail *systems* are the applications that enable users to compose, transmit, receive, and manage, text and/or graphic e-mail messages and images across LAN and WAN networks and through gateways connecting the latter with the Internet. Within Kentucky state government, the e-mail environment is almost exclusively Microsoft Exchange/Outlook-based.

E-mail *messages* are any communication supported by e-mail systems for the conduct of official agency business internally, between other state, local, and federal agencies, and externally with constituents, voters, vendors, clients, citizens, and others. This definition applies equally to the contents of the communication, the transactional information associated with each message, and any attachments to the body of the message.

E-mail *server* is the hardware on which the application resides. For most state agencies this server is housed and physically managed by the Governor’s Office for Technology (GOT). Messages stored on this server, however, belong to the agency. **Any open records requests for messages stored on these servers will be handled by the agency, not GOT**. For proper records management, e-mail messages need to be moved off of this server and stored in a secure environment under the agency’s control.

Transactional information is information about the e-mail message. It can include the name of the sender and all recipients, the date and time the message was created and sent, the host application that generated the message, and all of the systems and computers the message was routed through. Some or all of this metadata may or may not be a visible part of the message. The federal courts have ruled that this information is a vital part of the message itself,[3] an important consideration when storing e-mail messages.

III. Managing E-mail Messages as Public Records

E-mail messages are a form of business communication and they contain information about business activities which, like records in other formats, are subject to audit, open records requests, and to legal processes such as discovery and subpoena. E-mail messages sent or received in the course of business transactions are government records and must be retained and managed for as long as they are needed for administrative, fiscal, legal, or historical requirements.

---

[3] Armstrong v. Executive Office of the President, 1 F3d 127 (D.D.C. 1993)

1. Identification of E-mail messages

The first step after receiving a message is to determine if the message is an agency record and then establish what kind of record the message is. While the agency records officer should be the person coordinating the records management activities of the agency, the originator of the record, i.e., author of the message, and/or the recipient is usually the person who makes the initial retention decision based on the nature of the message within the scope of his or her responsibilities.

The first question that needs to be asked is, *“Is the e-mail related to agency business?”*

Figure 1.1 illustrates the steps in this process.

If the answer is “No” then the message is considered **non-record** material. Non-record material has nothing to do with the actions of the agency and should be deleted immediately. Examples may include:

> **Personal Messages** – Employees need to be reminded that the e-mail system is provided by the state for work use primarily. While a certain amount of personal material maybe acceptable, abuse of the system can lead to disciplinary action and even dismissal. All agencies should have an appropriate use policy that determines the amount of personal messages acceptable on the system. (See “Internet and Electronic Mail Acceptable Use Policy, CIO-060”)
>
> **“Spam”** is the term for electronic “junk” mail. It is similar to the advertising mail that you get at home. It is completely unsolicited and unwanted. Some spam mail can be offensive in nature and sent, by hackers, as a way of disrupting normal business operations. Spam is a growing problem in government e-mail accounts. While there are tools and techniques for restricting the amount of spam you receive, there are currently no ways to keep it out completely without interfering with the ability to receive important messages. Agencies should contact their IT staff if they are receiving large amounts of spam mail.
>
> **Unsolicited E-mail** could be considered a type of spam, but in this context is referring to mail that may be unwanted, but is somewhat business related such as advertising from vendors. This could also include non-work related e-mail from coworkers such as jokes, miscellaneous news articles, non-work related announcements, etc. As with personal messages, an agency e-mail use policy needs to spell out how much non-work related e-mail can be on the system.

If the message is business related, then the message needs to be classified as to the appropriate type of record and the proper retention period should be applied.

2. Value and Retention of E-mail Records

All e-mail messages do not have the same value to the agency, and therefore do not have the same retention period. The information in the e-mail, the reason it was created, and the administrative, fiscal, legal, and/or historical value of the e-mail to the agency determine what kind of record the message is. The majority of e-mail messages in most agencies are minor administrative records having only brief convenience or reference value. However, e-mail is used to transmit records having significant administrative, legal, research, or other value and may need to be retained long-term, and some may need to be retained permanently.

As public records, e-mail messages are subject to the same retention requirements as the same type of record in another format or medium. This means that e-mail messages must be retained and disposed of in the same manner as the agency's other records, according to the records retention schedule approved by the State Archives and Records Commission for that agency. Retention periods for e-mail records will vary according to the information the messages contain and the functions the messages perform. Just as an agency cannot schedule all paper or microfilm records together under a single retention period, an agency cannot simply schedule e-mail as a single record series.

Any record, paper or electronic, should not be destroyed if it is the subject of an open records request and/or legal action (i.e. discovery motion, subpoena, court order, etc.). Even if the retention period for the record allows for its destruction, it must be retained until the open records request (including any and all appeals) and/or the legal action is completed. Agencies should establish procedures for dealing with Open Records Requests (see Subsection 5. Accessibility of E-mail Messages.)

E-mail messages may have one of three different values depending on the information in and the function of the message to the agency. (Many of these types of records are found in the *General Schedule for State Agencies* or *The Local Government General Records Schedule* – although they may be covered in the agency-specific schedule also):

> **Informational and Reference Material** are transitory in nature, are of no meaningful value to an agency for documenting its policy, establishing guidelines or procedures, or to certify transactions and may be destroyed as soon as they are no longer needed. Most e-mail messages fall in this category. Some examples of these types of messages are communications received from a professional listserv (not used for project development or creation of policy); or, general announcements received by all employees such as news of an upcoming fire drill or impending building repair. These records can be disposed of when they are no longer needed as outlined in the schedule:
>
> *General Schedule for State Agencies: Miscellaneous Records:*
> series **M0018 Informational and Reference Material**
> Disposition: Destroy when no longer useful.

General Schedule for Local Agencies: Common Records, Administrative:
series **L4956 Informational and Reference Material**
Disposition: Destroy when no longer useful.

Temporary records have some documentary value to the agency, but do not need to be retained permanently. The retention period is determined by assessing their administrative, fiscal, or legal need. This time period may range from a few months to several years and should be defined in the agency's records schedule or the *General Schedule for State Agencies* or *The Local Government General Records Schedule*. These records must remain accessible for the *entire* retention period specified in the schedule. E-mail records in this category should be managed and maintained like the rest of the agency's temporary records. Some examples of temporary records are (from the *General Schedule for State Agencies* or *The Local Government General Records Schedule)*[*]

General Correspondence (series **M0002** state**; L4955** local)
Activity Report (series **M0029**)
Disposition: Retain for no longer than 2 years, destroy.
Meeting Notices (**L4953** local)
Disposition: Retain for I year, destroy.

Permanent records are programmatic records of the agency that have lasting historical value because they document the function and duties of the agency over time. For state agencies, these records may eventually be transferred to the Kentucky Department for Libraries and Archives for storage in the State Archives Center. Some examples of permanent records are (from the *General Schedule for State Agencies* or *The Local Government General Records Schedule)**

Official Correspondence – Having enduring historical or legal value (series **M0001; L4954** local)
Annual or Summary Reports (series **M0022** state**; L4951** local)

All e-mail messages must be reviewed and classified in a timely manner to ensure good records management practice throughout the enterprise. All agency employees who use e-mail must be trained in using the records retention schedules to identify the types of records they create and receive. **Non-business related and transitory e-mail messages should be removed from the e-mail system as soon as possible.** If this is done by the employee on a regular basis, then e-mail can be managed with relative ease. Agencies may find it helpful to have "file clean-up" or "file management" days on a periodic basis. These are selected days where employees are encouraged to go through their e-mail folders and clean out messages that have passed their retention period. This can be coordinated with "file clean-up" for paper records as well.

---

[*] The examples used here are records common to all agencies. Other types of e-mail records that are specific to the agency, may be found on the agency's records retention schedule.

3. Responsibility for Retention
Once it has been determined that an e-mail message is a record that needs be retained, you need to determine who in the agency, is the one responsible for retaining it; the sender or the recipient.

Figure 1.2 provides an outline for determining who has this responsibility for retaining the e-mail message.

If the message comes from outside of the agency, this record represents incoming correspondence and should be retained by the person in the agency who received the message and acted on it. An exception to this would be if someone else (such as another section or division) in the agency is responsible for handling the action required to deal with the e-mail, the initial recipient may forward it to that person, who would be responsible for filing the message.

If the message is sent and received by personnel within the same agency, not all of them need to retain a copy of the same message. If the message that was sent, was not altered in any way (responded to, edited, had attachments added, etc.) then the original sender has the responsibility for retaining the message. If a recipient did make alterations to a message, then the recipient would be responsible for retaining the message. If there is a string of multiple replies between two or more people to the same message, then only the last reply needs to be saved **only if all of the replies and comments are captured in the final message.** This is done by ensuring that the "include original message text" feature is activated for any replies and forwards.

4. Filing Structures. Employees should be trained in using the agency's e-mail application to create folders for organizing their e-mail messages. An organized system of folders helps individuals in separating informational, temporary, and permanent records and can help ensure that important records are not accidentally lost or misplaced. Folders are especially helpful if the individual's filing structure mirrors that of the agency, especially if the agency employs an electronic record keeping system[*]. The agency should develop a standardized system for naming files and folders to avoid confusion over the contents of a file.

Figure 1.3 provides a sample filing structure for an individual's e-mail account.

This should be a location on the agency's network that is secure and backed-up on a regular basis. All agencies need to establish logical and coherent filing structures and naming conventions for creating folders on the agency's network drive(s). An organized system of folders helps individuals in separating and classifying informational, temporary, and permanent records and can help ensure that important records are not accidentally lost or misplaced. Employees need to be trained in how to create folders in the e-mail application and where/how to place the folders on the network drive(s).

---

[*] In the context of this document an electronic record keeping system is an electronic system that stores and organizes electronic files for enhanced distribution and access. It can also be referred as a document management system.

These folders **should not be located on the individual's workstation** (their "C" drive). This is not a secure location and is not backed-up to protect from accidental loss. The folders should also not be located in the application's "In-box." These folders should be located in the folders created for that individual located on the agency network or in an electronic record keeping system if the agency employs one. (See IV. Preservation of E-mail Records, Near-line Storage.). Agencies should utilize their IT staff to assist with the proper placement of Outlook or other network folders.

5. Accessibility of E-mail Records. Because e-mail messages are public records, they are subject to the same open records requirements as any of the agency's other public records. The legal issues governing this access are frequently very complex. E-mail messages must be managed in such a way that agencies can respond promptly to open records requests.

E-mail messages that are available for public inspection, must remain accessible throughout their *entire* retention period and should be maintained in a manner which permits efficient and timely retrieval. Developing a standardized system of document naming, filing, indexing and retrieval (within the e-mail applicaiton or grouped together with other files in electronic record keeping systems), will assist an agency in maintaining the accessibility of non-exempt e-mail messages throughout the required retention period.

Appropriate measures should be taken by the agency's records custodian to insure that e-mail messages that are the subject of pending open records requests and/or litigation are not deleted from the e-mail, or other electronic record keeping system, before the request, and any appeals, are met. When the custodian is made aware of the request or litigation, agencies should generate a separate file that captures a complete copy of the appropriate e-mail message(s) and maintain that copy in a separate secure directory under the control of the designated records custodian for a period of 30 days or as long as the case is being litigated or appealed. Documentation of this procedure (date, time, and number of messages) should also be created and maintained as long as the file is maintained. Once a secure copy of the message(s) has been generated, the other copy can be handled according to the agency's records management procedures and with the principles spelled out in these guidelines.

Having e-mail messages that are inaccessible, either through hardware/software obsolescence or because of faulty indexing schemes, can be as problematic as inappropriately destroying the records and could expose the agency to legal risk. (See section 4 above for a sample filing structure.)

IV. Preservation of E-mail Records

Government agencies have the responsibility for developing guidelines and procedures to incorporate e-mail messages into their overall record-keeping systems following policies approved by the Kentucky Department for Libraries and Archives. Agency administrators should also develop policies and systems designs to ensure that e-mail records are appropriately preserved, secured, and made accessible throughout their established retention periods. Procedures and systems configuration will vary according to the agency's needs and particular hardware and software used.

Simply backing up the e-mail system onto tapes or other media or purging all messages after a set amount of time are not appropriate strategies for managing e-mail.

Agency records of long-term value should not be stored on individual workstations. The records should be stored on a secure drive that has the proper security features to protect the records from alteration or destruction and to provide regular back-up. Offsite employees with laptops should download their messages to the agency's network drives on a regular schedule.

There are three ways to preserve e-mail messages: on-line, near-line, and off-line. All of the methods have advantages and disadvantages that must be considered before determining which is right for the agency.

1. On-line Storage

On-line storage maintains e-mail messages in the e-mail application itself. This is a good method for storing temporary and short-term records (less than 5 year retention). Microsoft Outlook does have limited capability which can be employed by using the "archiving" function in the application.

There are several advantages to storing e-mail messages in the e-mail application. The messages can be searched and retrieved quickly and easily with electronic indexing. The dynamic functionality of the messages can be retained, and the messages can be stored in their native format. Since the agency already has the e-mail application in place, the costs are less than running the e-mail application with a parallel system.

Messages must be moved off the main e-mail server and into a secure drive or the application will not respond properly and messages could be lost.

2. Near-line Storage

Near-line storage involves the transfer of the e-mail messages and transactional information into an electronic record keeping system, other than the e-mail system itself. For example, an e-mail message dealing with a particular project could be stored in a file on the agency's network drive with other electronic files dealing with the same project. The message still retains some of its functionality, including the ability to be indexed and retrieved electronically. If the agency stores other records in electronic format, then the e-mail messages can be integrated with other related project files.

Disadvantages to storing records near-line are the potential costs for the equipment, maintenance and service for the electronic record keeping system. The agency should consider the costs and benefits, and the compatibility of their e-mail application and the electronic record keeping system. Storing messages external to the e-mail application may mean converting the messages to a different format, which could result in the loss of important information. Records with retention periods of more than 5 years need to be migrated and possibly converted to new formats and systems as older ones become outdated. Finally, if the agency still maintains many of its records in paper, then the two systems (paper filing system and the electronic system) must be integrated and work together.

3. Off-line (Paper) Systems

In some cases, especially for permanent and long-term (greater than 10-15years) records, the best preservation solution may be to print the e-mail messages, and transactional information, onto paper. This solution makes sense if the agency does not already have an electronic system in place that is designed for long-term records protection and accessibility or if a majority of its records are kept in paper form.

The biggest advantage to off-line storage is the stability of the medium. Agencies do not have to worry about hardware and software becoming outdated and the records becoming irretrievable. E-mail messages can be filed with other records of the same type or series directly, making the retention and disposition process easier.

The disadvantage is that the e-mail messages lose their dynamic functionality as electronic documents. They cannot be searched and retrieved as quickly and efficiently as in a well-managed electronic system. Finally, with the pervasive use of e-mail applications in the course of government business, the volume of paper records will build up quickly.

Note: No matter what storage option the agency chooses, transactional metadata *must* be properly captured and stored with the e-mail message for the full value of the document to be preserved. This task is usually easy in e-mail applications that readily display this information. Applications that do not display the metadata need to be configured so that the data stays with the message in whatever form the message is retained.

VI. Other Management Considerations for E-mail Systems

Electronic systems share some of the same management concerns as off-line (paper) systems. Below are some considerations to help agency officials on overall management of e-mail records.

Transactional information (metadata)

This data is the information about the e-mail message that accompanies the message for routing, tracking, and usage purposes. It can include the name of the sender and all recipients, the date the message was created and sent, information about the host application that generated the message, and a record of all of the systems and computers the message was routed through. In some e-mail applications, this metadata is a visible part of the message; in some applications it is in the header; and in some other applications, the metadata is stored in a "properties" file. Transactional information is an important consideration in any information system for retention of e-mail and any legal use that maybe made of an e-mail message.

Distribution lists

In a distribution list, groups of recipients that are referenced under a common name. For instance, if an employee is a member of a planning committee, then a list can be created that contains the e-mail addresses of all of the members of that committee; to send a message to the entire committee, the list name is typed into the "To" line of the message, rather than each individual address. If such lists are used, then the names and addresses of all the list members need to be retained along with the message, if that information is important to the evidentiary value of the message. For example, knowing that a message was sent to "Budget Committee" but not knowing the names of the recipients omits part of a documentary function the message was intended to serve.[*]

Back-ups and System Security.

Electronic storage systems should be backed up regularly to protect from system failures, unintentional deletions, or tampering. Routine back-up procedures are for emergency recovery purposes, however, and do not constitute a long-term record keeping solution for e-mail. Recovering messages from back-up tapes can be problematic and many tapes are re-used repeatedly.

Agencies should develop procedures to provide for the security of e-mail records so that they cannot be altered or deleted, intentionally or unintentionally. This security is important to ensure that the e-mail records remain reliable and authentic evidence of the agency's activity, for regulatory, auditing and legal accountability. The agency needs to document its procedures for handling and securing agency e-mail, who has access to the system, and maintain an audit trail tracking any alterations to messages in the system.

Deletion of E-mail Messages

Non-permanent records should be deleted when the proper retention period has expired. Simply deleting the message *does not* necessarily remove it from the hard drive or server, however. Utility programs that can be purchased to make sure hard drives are wiped clean and the messages are completely removed. This will eliminate wasted storage space and help avoid legal consequences if deleted messages are recovered. As with any of these procedures, the destruction policy needs to be well documented and followed by all levels of the agency.

---

[*] Ad-hoc lists created in an individual's "Contacts" folder put the individual addresses in the message. However, lists that are on the global list in Exchange only put the name of the list on the message. One work around for this is for the sender to "BCC" themselves and they will receive a message with all of the addresses listed that can filed or record keeping purposes.

Expired messages should be removed from back-up tapes of both the e-mail server and from any other electronic record keeping system the agency may employ. Even if the e-mail messages have been properly deleted from the electronic files, messages on back-up tapes are still discoverable and could present legal liability to the agency.

Control of Copies

Because e-mail messages can be forwarded and routed to multiple addresses, copies of the messages could exist after the retention period has expired. All agency staff should be trained in identifying what constitutes the official, or “record” copy. In most cases, the author or creator and/or the principal recipient of the e-mail message is responsible for maintaining the record copy, but the retention for other copies is governed by the function the record plays in documenting the work of the recipient. Employees should be encouraged to delete unofficial copies of messages as soon as possible.

When an Employee Leaves

Any time an employee leaves an agency the employee’s e-mail messages need to be reviewed by the appropriate personnel to ensure that any records are properly classified and stored, and that any non-records are disposed of in the correct manner. **This should be done before the former employee’s account is removed from the e-mail server.** Ideally, the employee would be doing this type of file management on a regular basis, just as they do with paper files. Employee exit procedures, however, should verify that records remaining in an email account are appropriately transferred to others within the organization or deleted, as is dictated by retention schedules.

If the employee had personal messages on the e-mail system, the agency is under no obligation to retain that information. However, in cases where the employee was dismissed or demoted due to misuse of the e-mail system, these messages may be used as evidence by the agency or the employee in responding to the charges. While the agency is not obligated to retain non-business related material, it cannot destroy evidence, and may be required to allow the employee access to these messages in order to rebut the charges.

Agencies should, in consultation with their legal counsels, come up with written procedures for the handling of the e-mail accounts of dismissed employees. The procedures should include:

1. How the dismissed employee's account will be handled. (The messages could be filed off to a secure folder on the agency's network drive, CD-ROM, etc.)

2. Who will review the messages. This should be someone in the agency who is familiar with the records that could be in the employee's e-mail account and has the authority to make decisions about deleting records.

3. State agencies should retain the messages in the employee's account for, at least 61 days to allow for appeals of disciplinary actions to the state Personnel Board. Local agencies should retain the messages for the appropriate amount of time the employee has to appeal the dismissal. Once an appeal is made, then messages must be retained for the duration of any legal investigation, audit, lawsuit or administrative hearing.

4. If no appeal is made in the appropriate time period, then the non-record messages may be deleted.

VII. Employee Training

All agency employees should be trained in using the records retention schedule to identify and classify the records they create. They should be aware of proper retention and disposition procedures and of who to contact when records need to be transferred out of their custody. Because individual employees have direct control over the creation and distribution of e-mail messages, agencies should provide training for their employees on agency e-mail procedures. Depending on the type of e-mail and record keeping system an agency uses, policies and procedures will vary.

In addition to those mentioned previously, the following issues should be addressed in any e-mail policy:

1. **Appropriate Usage of E-mail Systems.** The e-mail system is provided, at the agency's expense, to assist employees in carrying out government business. The e-mail system is property of the agency and the agency has the right to monitor and review the use of the system. The courts have been fairly consistent about the use of computing resources at the workplace, especially the government workplace, for personal transactions: these transactions are not private, nor do they belong to the individual.[4] E-mail should be used only to transmit business related information. Every agency should develop a written policy statement for its employees regarding appropriate usage of an e-mail system. The Enterprise "Internet and Electronic Mail Acceptable Use Policy (CIO-060)" provides the minimum requirements for state agencies to follow and can serve as a model for local agencies in developing their own use policy.

---

[4] "Electronic Records Draft Guidelines, Part 4: E-mail," Mississippi Department of Archives and History, [Internet document accessed on 5-22-2002], 1.

2. **E-mail Confidentiality/Privacy.** E-mail messages travel through several computers and networks and could be captured and viewed at any point along the way. E-mail communication should be used with the assumption that a message might be read by many people, not just the intended recipient. Sensitive, or confidential information should not be transmitted via e-mail unless the proper protocols have been followed to secure the message. (See 5. Encryption below)

   Because e-mail has become such a commonly used business communication tool, care needs to be taken to protect personal privacy rights of other coworkers (or any other third party). While information of a personal nature (social security numbers, home phone numbers and addresses, medical conditions, etc.) should not be included in e-mail messages, it is unreasonable to expect staff to not use the benefits of the messaging system for this type of communication. While these messages are usually exempt from open records requests, they could be stored in an in-box with non-exempt messages and exposed inadvertently.

3. **Subject Lines**. Proper use of clear and concise subject lines helps in identifying the content of e-mail messages and in indexing and retrieving e-mail messages stored in electronic record-keeping systems. Clear, concise subject lines are also a courtesy for the recipient in identifying important messages from the sea of unimportant junk, or "spam," mail that a person may receive. A good subject line should be as descriptive as possible about the content of the message. Below are some examples of good and bad subject lines.

Poor or confusing subject lines[5]	Good or descriptive subject lines
"helpful info"	"contact info"
"report"	"quarterly financial report"
"minutes"	"Jan 99 board minutes"
"important"	"revised admin. procedures"
"today?"	"lunch plans today?"
"news"	"new agency head appointed"

---

[5] "Managing Electronic Mail: Guidelines for State of Ohio Executive Agencies," Electronic Records Committee, Ohio State Historical Society, April 2000, 7.

4. **Viruses.** Government agencies are one of the most popular targets for people trying to disrupt computer systems. Many viruses can be attached to e-mail messages sent to government recipients without the sender's knowledge. Agency staff members may even receive viruses from someone they know and trust. Agencies should establish policies regarding the opening of e-mail attachments and for system security.

5. **Encryption.** Because encryption can complicate long-term storage of e-mail, it should only be used when the function of the message dictates the need and when methods exist to decrypt. If used, the encryption method must follow established state guidelines and procedures.

This discussion covers only the most basic issues involved in a very complex subject. In preparing e-mail policies and procedures, agencies should involve the agency's information technology, records management, and legal counsel staff.

References

"Developing E-Mail Policy for Government Agencies." *Government Records News.* 1 (December 1996).

"Guideline for Managing E-mail." ARMA International. 2000.

Electronic Records Draft Guidelines, Part 4: E-mail," Mississippi Department of Archives and History, [Internet document accessed on 5-22-2002]

"Managing Electronic Mail: Guidelines for State of Ohio Executive Agencies." Ohio State Historical Society. April 2000. http://www.ohiojunction.net/erc/e-mail/e-mailguidelines.html

"Managing E-mail." Public Records Information Leaflet No. 21. South Carolina Department of Archives and History. April 1998.

"Managing Records in E-Mail Systems," New York State Archives and Records Administration (NYSARA) 1995.

Figure 1.1
Decision Sequence for Determining E-Mail Retention

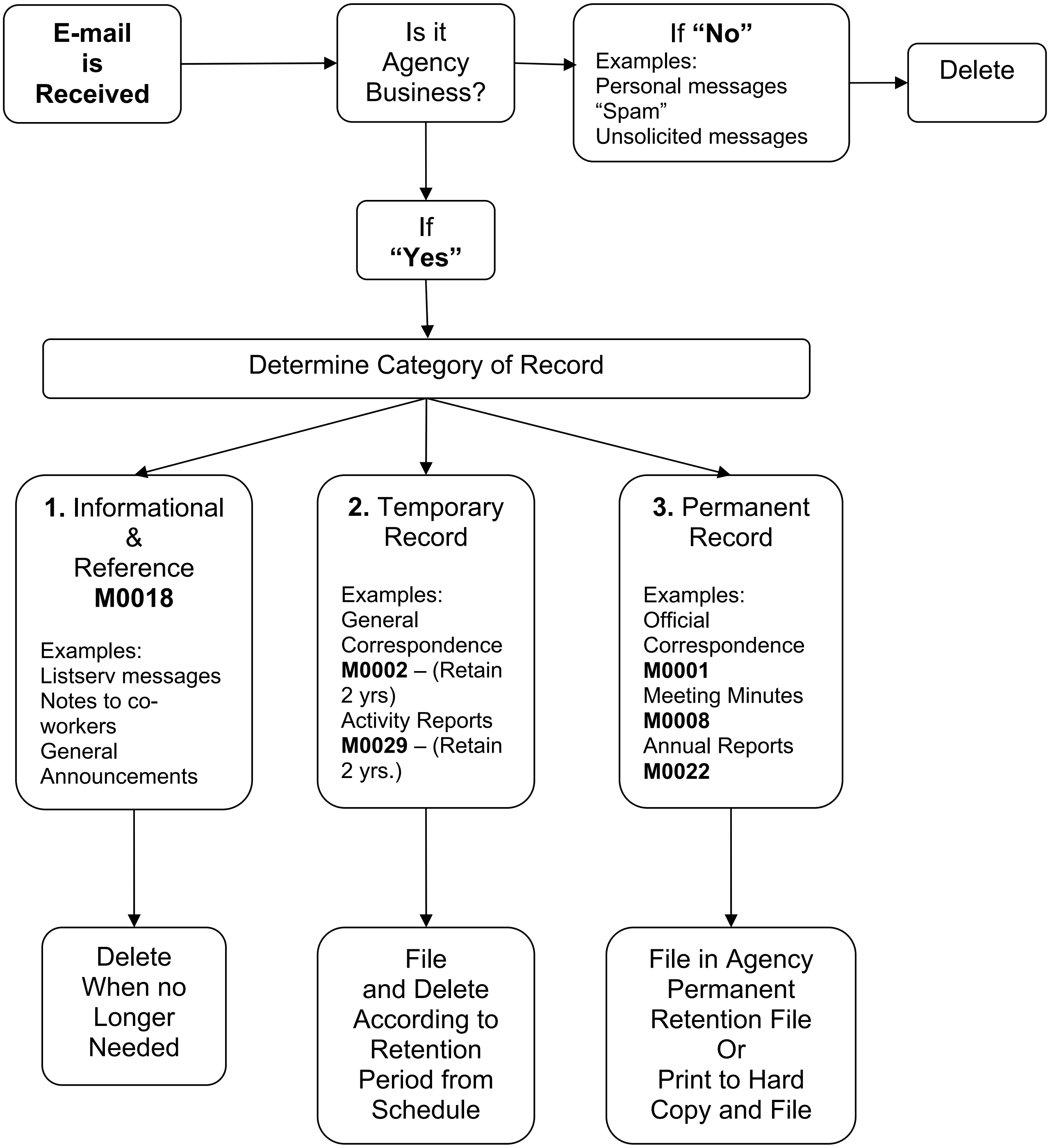
E-mail is Received
Is it Agency Business?
If "No"
Examples:
Personal messages
"Spam"
Unsolicited messages
Delete
If "Yes"
Determine Category of Record
1. Informational & Reference M0018
Examples:
Listserv messages
Notes to co-workers
General Announcements
2. Temporary Record
Examples:
General Correspondence
M0002 – (Retain 2 yrs)
Activity Reports
M0029 – (Retain 2 yrs.)
3. Permanent Record
Examples:
Official Correspondence
M0001
Meeting Minutes
M0008
Annual Reports
M0022
Delete When no Longer Needed
File and Delete According to Retention Period from Schedule
File in Agency Permanent Retention File Or Print to Hard Copy and File

Figure 1.2 Determining Responsibility for Retaining E-Mail Messages

Because e-mail messages can be forwarded and routed to multiple addresses, copies of the messages may exist in many areas of the agency. In most cases, the author, or originator, of the e-mail message is responsible for maintaining the "record" copy. However, in cases in which the recipient has altered the message (made changes, added attachments, etc.), or when the message is coming from outside the agency (and therefore not documented anywhere within the agency), the recipient is the one responsible for retaining the message.

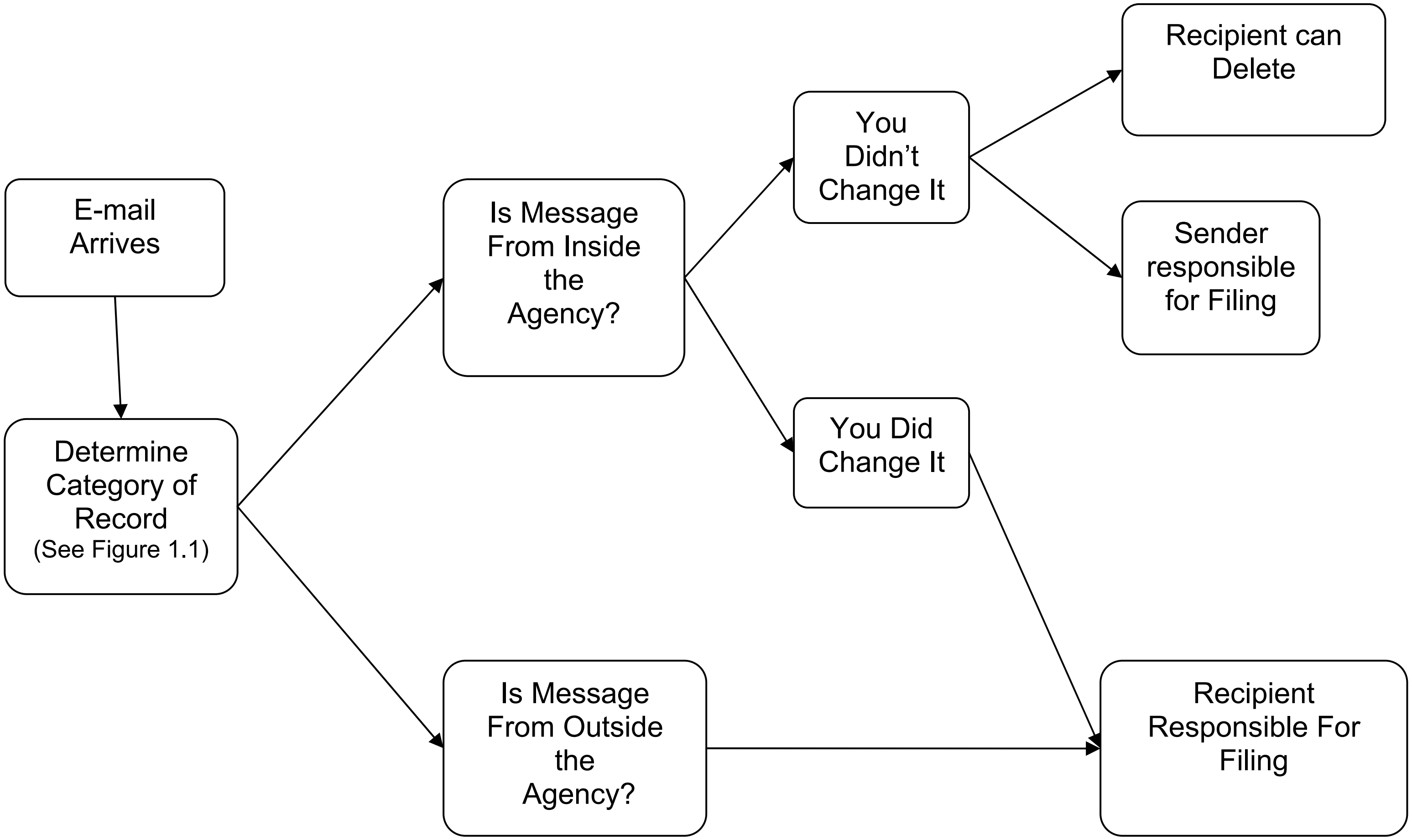
E-mail Arrives
Determine Category of Record (See Figure 1.1)
Is Message From Inside the Agency?
Is Message From Outside the Agency?
You Didn't Change It
You Did Change It
Recipient can Delete
Sender responsible for Filing
Recipient Responsible For Filing

Figure 1.3

Sample Filing Structure for E-mail

The following is an example of an agency filing structure for e-mail. The records series numbers, from the *General Schedule for State Agencies**, are provided in parentheses.

NON-RECORD MESSAGES – Delete at will

- **Personal Messages** – (An agency appropriate use policy should detail the amount of personal messages allowed on the e-mail system.)
- **"Spam"/ Unsolicited e-mail**

INFORMATIONAL AND REFERENCE MATERIAL – (M0018) Delete when no longer useful.

- **Drafts** – Publications, Reports, Memos
- **Meeting Notices**
- **Listserv Messages**

TEMPORARY MESSAGES – Delete per Retention Schedule*

- **General Correspondence** (M0002 – delete after 2 years)
  - Project 1
  - Project 2
  - Person A (Supervisor)
  - Person B (Co-worker)

- **Activity Reports** (M0029 – delete after 2 years)
  - Year #
    - Jan, Feb, etc.

PERMANENT MESSAGES – (As defined by retention schedules*) Check with agency records officer for appropriate filing procedures.

- **Official Correspondence** (M0001 – usually from agency or division head)
  - Project A
  - Project B
- **Annual or Summary Reports** (M0022)
- **Policies and Procedures** (M0003 – final copy)
- **Meeting Minutes (Board or Commission)** (M0008)

*These examples come from the *General Schedules for State Agencies*, more records categories can be found in the agency-specific schedule.